

THE HIGH COURT

[2013 No. 765JR]

BETWEEN/

MAXIMILLIAN SCHREMS

APPLICANT

AND

DATA PROTECTION COMMISSIONER

RESPONDENT

REQUEST FOR A PRELIMINARY RULING

ARTICLE 267 TFEU

To:

The Registrar,

Court of Justice of the European Union

L-2925 Luxembourg

The High Court of Ireland (Mr. Justice Gerard Hogan) hereby refers the questions set out at paragraph 22 below to the Court of Justice for preliminary ruling in accordance with Article 267 TFEU.

Introduction

1. The questions referred arise in judicial review proceedings before the High Court in which the above-named applicant, an Austrian national, challenges a decision of the respondent Data Protection Commissioner (“the Commissioner”) not to investigate his complaint further pursuant to s. 10(1)(b) of the Data Protection Act 1988 (“the 1988 Act”). A copy of the proceedings booklet is attached at **Appendix 1**. A consolidated version of the Data Protection Acts 1988-2003 is attached at **Appendix 2**.

2. All users in Europe of the major social network, Facebook, are required to sign a contract with Facebook Ireland Ltd. (“Facebook Ireland”). To that extent, therefore, Facebook Ireland falls to be regulated by the Commissioner under the Irish Data Protection Acts. Facebook Ireland is a subsidiary of its US parent, Facebook Inc. (“Facebook”). Mr. Schrems has been a user of this social network since 2008. Some or all data relating to Facebook subscribers residing within the EU/EEA is in fact transferred to and held on servers which are physically located within the United States.

3. The essence of Mr. Schrems’ complaint of 25th June, 2013, to the Commissioner was that in the light of the revelations made from May, 2013 onwards by Edward Snowden concerning the activities of the US National Security Agency (“NSA”), there was no meaningful protection in US law and practice in respect of data so transferred to the US so far as State surveillance was concerned.

4. By letters dated 25th and 26th July, 2013, the Commissioner invoked his power under s. 10(1)(a) of the 1988 Act not to investigate this complaint further on the ground that this complaint was frivolous and vexatious: see paras. 30 and 31 of the judgment delivered on 18th June, 2014, a copy of which is set out at **Appendix 3**. As a matter of Irish law and in this particular statutory context these words simply mean that the Commissioner concluded that

the claim was unsustainable in law. Specifically, contrary to the argument urged by the applicant, they bear no other connotation: see paras. 34-40 of the judgment.

5. The reason why the Commissioner reached this conclusion was because (i) there was no evidence that Mr. Schrems' personal data had been so accessed by the NSA (or other US security agencies) ("the *locus standi* objection"), so that the complaint was purely hypothetical and speculative and (ii) because the European Commission had determined in its decision of 26th July, 2000 (2000/520/EC) ("the Safe Harbour Decision") that the United States "ensures an adequate level of [data] protection" in accordance with Article 25(6) of Directive 95/46/EC ("the 1995 Directive"). The Commissioner noted that the Safe Harbour decision was a "Community finding" for the purposes of s. 11(2)(a) of the 1988 Act, so that any question of the adequacy of data protection in that third country (in the present case, the United States) where the data is to be transferred was required by Irish law "to be determined in accordance with that finding." As this was the gist of the applicant's complaint – namely, that personal data was being transferred to another third country which did not in practice observe these standards – the Commissioner took the view that this question was foreclosed by the nature of the Safe Harbour Decision.

The *locus standi* objection

6. The Commissioner maintained that Mr. Schrems had no *locus standi* to make this complaint. As he could not show that his personal data had been so accessed by the NSA, it was said that he complaint was essentially hypothetical and speculative. While I accepted (see paragraphs 41-45 of the judgment) that Mr. Schrems could not say whether his own personal data has ever been accessed or whether it would ever be accessed in this fashion by the US authorities. But even if this were considered to be unlikely, I held that he was nonetheless "certainly entitled to object to a state of affairs where his data are transferred to a jurisdiction which, to all intents and purposes, appears to provide only a limited protection

against any interference with that private data by the US security authorities.” I accordingly rejected the *locus standi* objection.

The evidence and the findings of fact

7. I found the following facts regarding the interception of personal data:

- (a) Electronic surveillance and interception of communications in the manner provided by law serves necessary and indispensable objectives which are in the public interest, namely, the preservation of national security and the prevention of serious crime. The surveillance and interception of personal data transferred from the EU to the US by the US National Security Authority (and other similar agencies, both in the US and elsewhere) serves legitimate and necessary counter-terrorism objectives and goals.
- (b) Nevertheless, the revelations made by Edward Snowden demonstrated a significant over-reach on the part of those authorities. While there is oversight on the part of the Foreign Intelligence Services Court in the US, this is done on an *ex parte* and secret basis. EU citizens have no effective right to be heard on the question of the interception and surveillance of their data and, furthermore, decisions taken to access such data are not conducted on the basis of EU law.
- (c) While there may be some dispute regarding the scope and extent of some of these programmes, it is from the extensive exhibits contained in the affidavits filed in these proceedings that the accuracy of much of the Snowden revelations does not appear to be in dispute. I accordingly found that personal data transferred by companies such as Facebook Ireland to its parent company in the United States is thereafter capable of being accessed by the National

Security Authority (and other federal agencies such as the Federal Bureau of Investigation) in the course of a mass and indiscriminate surveillance and interception of such data. Indeed, in the wake of the Snowden revelations, the available evidence presently admitted of no other realistic conclusion: see paragraphs 10-13 of the judgment.

- (d) Both Facebook and Facebook Ireland had self-certified pursuant to the Safe Harbour decision.

National law

8. Irish national law precludes the transfer of personal data outside of the State, save where that foreign State “ensures an adequate level of protection for the privacy and the fundamental rights and freedoms of data subjects in relation to the processing of personal data having regard to all the circumstances surrounding that transfer.” I found that the standards referred to here are those contained in the Constitution of Ireland 1937: see paragraph 20 of the judgment.

9. As far as Irish law is concerned, the accessing of private communications by the State authorities through interception or surveillance engages the constitutional right to privacy. Further, accessing by State authorities of private communications generated within the home – whether this involves the accessing of telephone calls, internet use or private mail – is also a clear interference with the inviolability of the dwelling as guaranteed by Article 40.5 of the Constitution: see paras. 47 and 48 of the judgment. Copies of the relevant Irish case-law are included in **Appendix 4**.

10. I further held that the mere fact that these rights are thus engaged does not mean that the interception of communications by State authorities is necessarily or always unlawful. The Preamble to the Constitution of Ireland envisages a “true social order” where the “dignity

and freedom of the individual may be assured”, so that both liberty and security are valued. Provided appropriate safeguards are in place, I ruled that in a modern society electronic surveillance and interception of communications is indispensable to the preservation of State security. It was accordingly plain that legislation of this general kind serves important – indeed, vital and indispensable – State goals and interests, drawing by analogy on the decision of the German Constitutional Court in the *Anti-Terrorism Database* case (April 24, 2003)(at paras. 106, 131 and 133, *passim*) and the comments of this Court in Case C-293/12 *Digital Rights Ireland Ltd.* [2014] E.C.R. I-000 at paras. 42-44.

11. I further held that the importance of these constitutional rights is such nonetheless that the interference with these privacy interests must be in a manner provided for by law and any such interference must also be proportionate. This is especially the case in respect of the interception and surveillance of communications within the home. While the use of the term “inviolable” in respect of the dwelling in Article 40.5 of the Constitution not literally mean what it says (*i.e.*, so that the right was not absolute or incapable of being interfered with), the reference to inviolability in this context nonetheless conveys that the home enjoys the highest level of protection which might reasonably be afforded in a democratic society: see paras. 49-50 of the judgment.

12. I then held the mass and undifferentiated accessing of personal data generated perhaps especially within the home – such as e-mails, text messages, internet usage and telephone calls – would not pass any proportionality test or could survive constitutional scrutiny on this ground alone. The potential for abuse in such cases would be enormous and might even give rise to the possibility that no facet of private or domestic life within the home would be immune from potential State scrutiny and observation. Such a state of affairs would be totally at odds with the basic premises and fundamental values of the Constitution: respect for human dignity and freedom of the individual (as per the Preamble to the Constitution);

personal autonomy (Article 40.3.1 and Article 40.3.2); the inviolability of the dwelling (Article 40.5) and protection of family life (Article 41). Drawing on earlier case-law (*The People v. O'Brien* [2012] IECCA 68), I noted that Article 40.5 of the Constitution presupposes that “in a free society the dwelling is set apart as a place of repose from the cares of the world” and assures “the citizen that his or her privacy, person and security will be protected against all comers”, save in a manner provided for by a law which respected the essence of that constitutional guarantee.

13. I then held that dwelling could not in truth be a “place of repose from the cares of the world” if, for example, the occupants of the dwelling could not send an email or write a letter or even conduct a telephone conversation if they were not protected from “the prospect of general or casual State surveillance of such communications on a mass and undifferentiated basis.” I then went on to say:

“That general protection for privacy, person and security in Article 40.5 [of the Constitution of Ireland] would thus be entirely compromised by the mass and undifferentiated surveillance by State authorities of conversations and communications which take place within the home. For such interception of communications of this nature to be constitutionally valid, it would, accordingly, be necessary to demonstrate that this interception of communications and the surveillance of individuals or groups of individuals was objectively justified in the interests of the suppression of crime and national security and, further, that any such interception was attended by appropriate and verifiable safeguards.”

14. I further held that if this matter were entirely governed by Irish law, then, measured by these particular constitutional standards, then at the very least a significant issue would arise as to whether the United States “ensures an adequate level of protection for the privacy and the fundamental rights and freedoms” within the meaning of s. 11(1)(a) of the 1988 Act,

such as would permit data transfers to that country. Moreover, given the (apparently) limited protection given to data subjects by contemporary US law and practice so far as State surveillance is concerned, this would indeed have been a matter which the Commissioner would have been obliged to investigate.

15. Accordingly, if the matter were to be judged *solely* by reference to Irish constitutional law standards, the Commissioner could not properly have exercised his s. 10(1)(a) powers to conclude in a summary fashion that there was nothing further to investigate.

National law pre-empted by European Union law: the Safe Harbour Decision

16. The parties were agreed, however, the matter is only partially governed by Irish law and that, in reality, on this key issue of the adequacy of data protection law and practice in third countries, Irish law has been pre-empted by general EU law in this area. This is because s. 11(2)(a) of the 1988 Act (as substituted by s. 12 of the Data Protection (Amendment) Act 2003) effects a *renvoi* of this wider question in favour of EU law. Specifically, s. 11(2)(b) of the 1988 Act provides that the Commissioner must determine the question of the adequacy of protection in the third State “in accordance” with a Community finding made by the European Commission pursuant to Article 25(6) of the 1995 Directive.

17. I next held that given that the validity of the administrative decision taken by the Commissioner not to investigate the matter further was contingent on the proper interpretation and application of the 1995 Directive and, indeed, a European Commission Decision taken pursuant to that Directive, this was a matter concerning the implementation of the EU law by a Member State within the meaning of Article 51(1) of the Charter, sufficient - at least so far as this part of the case is concerned - to trigger the application of the Charter: see, *e.g.*, Cases C-411/10 and C-493/10 *N.S.* [2011] E.C.R. I - 13991, paras. 64-69; see paragraph 60 of the judgment.

18. I then held (at paragraphs 64-70 of the judgment) that:

“64. This brings us to the nub of the issue for the Commissioner. He is naturally bound by the terms of the 1995 Directive and by the 2000 Commission Decision. Furthermore, as the 2000 Decision amounts to a “Community finding” regarding the adequacy of data protection in the country to which the data is to be transferred, s. 11(2)(a) of the 1988 Act (as amended) requires that the question of the adequacy of data protection in the country where the data is to be so transferred “shall be determined in accordance with that finding.” In this respect, s. 11(2)(a) of the 1988 Act faithfully follows the provisions of Article 25(6) of the 1995 Directive.

65. All of this means that the Commissioner cannot arrive at a finding inconsistent with that Community finding, so that if, for example, the Community finding is to the effect that a particular third party state has adequate and effective data protection laws, the Commissioner cannot conclude to the contrary. The Community finding in question was, as we have already seen, to the effect that the US does provide adequate data protection for data subjects in respect of data handled or processed by firms (such as Facebook Ireland and Facebook) which operate the Safe Harbour regime.

66. It follows, therefore, that if the Commissioner cannot look beyond the European Commission’s Safe Harbour Decision of July 2000, then it is clear that the present application for judicial review must fail. This is because, at the risk of repetition, the Commission has decided that the US provides an adequate level of data protection and, as we have just seen, s. 11(2)(a) of the 1998 Act (which in turn follows the provisions of Article 25(6) of the 1995 Directive) ties the Commissioner to the Commission’s finding. In those circumstances, any complaint to the Commissioner concerning the transfer of personal data by Facebook Ireland (or, indeed, Facebook)

to the US on the ground that US data protection was inadequate would be doomed to fail.

67. This finding of the Commission is doubtless still true at the level of consumer protection, but, as we have just seen, much has happened in the interval since July 2000. The developments include the enhanced threat to national and international security posed by rogue States, terrorist groupings and organised crime, disclosures regarding mass and undifferentiated surveillance of personal data by the US security authorities, the advent of social media and, not least from a legal perspective, the enhanced protection for personal data now contained in Article 8 of the Charter.

68. While the applicant maintains that the Commissioner has not adhered to the requirements of EU law in holding that the complaint was unsustainable in law, the opposite is in truth the case. The Commissioner has rather demonstrated scrupulous steadfastness to the letter of the 1995 Directive and the 2000 Decision.

69. The applicant's objection is, in reality, to the terms of the Safe Harbour Regime itself rather than to the manner in which the Commissioner has actually applied the Safe Harbour Regime. There is, perhaps, much to be said for the argument that the Safe Harbour Regime has been overtaken by events. The Snowden revelations may be thought to have exposed gaping holes in contemporary US data protection practice and the subsequent entry into force of Article 8 of the Charter suggests that a re-evaluation of how the 1995 Directive and 2000 Decision should be interpreted in practice may be necessary. It must be again stressed, however, that neither the validity of the 1995 Directive nor the validity of the Commission's Safe Harbour decision have, as such, been challenged in these proceedings.

70. Although the validity of the 2000 Decision has not been directly challenged, the essential question which arises for consideration is whether, *as a matter of European Union law*, the Commissioner is nonetheless absolutely bound by that finding of the European Commission as manifested in the 2000 Decision in relation to the adequacy of data protection in the law and practice of the United States having regard in particular *to the subsequent entry into force of Article 8 of the Charter*, the provisions of Article 25(6) of the 1995 Directive notwithstanding. For the reasons which I have already stated, it seems to me that unless this question is answered in a manner which enables the Commissioner either to look behind that Community finding or otherwise disregard it, the applicant's complaint both before the Commissioner and in these judicial review proceedings must accordingly fail."

19. Given that the critical issue in the present case was whether US law and practice afforded sufficient data protection¹ and that no issue was ever raised in these proceedings concerning the actions of Facebook Ireland/Facebook² *as such*³, I took the view that the real question was whether the Commissioner was bound by the earlier findings to this effect by the European Commission in the Safe Harbour Decision. In other words, this was really a complaint concerning *the terms* of that decision, rather than the manner in which the Commissioner *had applied it*: see paragraph 69 of the judgment. While Article 3(b) of the Safe Harbour Decision allows the national authorities to direct an entity to suspend data flows to that third country, this is in circumstances where - unlike the present case - the complaint is

¹ Thus, the key ground advanced by the applicant (ground no. 3) in his Statement of Grounds dated 21st October 2013 (i.e., the document which forms the basis for the judicial review proceedings) was to the effect that in the light of the recent Snowden revelations "and the making available on a large scale of private data to the [US] intelligence services", the Commissioner could not properly have concluded that "in the United States of America an adequate level of protection was in place."

² Mr. Schrems has made 22 separate complaints to the Commissioner concerning Facebook, but none of these complaints arose for consideration in the present judicial review proceedings.

³ Other than that they co-operated with the US security authorities under the PRISM programme by forwarding their user data and by granting "mass access" to such data without any need for probable cause: see complaint of June 25, 2013; affidavit of Maximilian Schrems, 21st October 2013, exhibit "MS 4".

directed to *the conduct of that entity*. Here the real objection is not to the conduct of Facebook as such, but rather to the fact that the Commission has already determined that the US law and practice provides adequate data protection in circumstances where it is clear from the Snowden disclosures that personal data of EU citizens so transferred to the US can be accessed by the US authorities on a mass and undifferentiated basis.

20. It must be stressed that neither the validity of the 1995 Directive nor the 2000 Safe Harbour decision were, as such, challenged in these proceedings. Nor has it been suggested that s. 11(2)(a) of the 1988 Act (as amended) does not faithfully reflect the terms of Article 25(6) of the 1995 Directive.

21. In these circumstances I took the view that it would be appropriate that I should refer the question of whether, having regard in particular to my earlier findings of fact regarding the Snowden disclosures and the subsequent entry into force of Article 7 and Article 8 of the Charter and the recent judgment of this Court in *Digital Rights Ireland*, the Commissioner was bound by the earlier determination of the European Commission in the Safe Harbour Decision as to the adequacy of the data protection offered by US law and practice.

The questions referred

22. It was in these circumstances, accordingly, that I referred the following questions to the Court:

“Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in Commission Decision of 26 July 2000 (2000/520/EC) having

regard to Article 7, Article 8 and Article 47⁴ of the Charter of Fundamental Rights of the European Union (2000/C 364/01), the provisions of Article 25(6) of Directive 95/46/EC notwithstanding? Or, alternatively, may and/or must⁵ the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission Decision was first published?”

The views on the referring Court on the referred questions

23. Viewed in the abstract, it is hard to see how the Safe Harbour decision can in practice satisfy the requirements of Article 7 and Article 8 of the Charter, especially having regard to the principles articulated by the Court of Justice in *Digital Rights Ireland*⁶. Under this self-certification regime, personal data is transferred to the United States where it can be potentially accessed on a mass and undifferentiated basis by the US security authorities. No oversight is carried out on European soil and the data subject has no effective possibility of being heard or making submissions and, further, where any such review is not carried out by reference to EU law are all considerations which would seem to pose considerable legal difficulties: see paragraph 62 of the judgment.

24. Further, while it may be acknowledged that Article 7 of the Charter merely guarantees “respect” for the home - and in that regard may not go quite so far as Article 40.5 of the Constitution of Ireland which describes the dwelling as “inviolable” - it is nonetheless suggested the idea of the home as a place of sanctuary and, adapting the language of the Irish courts, a “place of repose from the cares of the world”, are critical elements of the guarantee of “respect” for the home and communications in Article 7 of the Charter and, in that respect, reflects core values common to the constitutional traditions of the Member States. That

⁴ At a further post-judgment hearing held on 2nd July 2014, it was agreed to amend the draft question to include a reference to Article 47.

⁵ The words “and/or must” were added at the suggestion of the applicant at the post-judgment hearing on 2nd July 2014.

⁶ See paragraphs 65-69 of the judgment.

guarantee would be wholly compromised if it were thought that electronic communications often emanating within the home could be accessed by State authorities (whether within the territory of the EU or by the authorities of a third country) on a causal and generalised basis without the need for objective justification based on considerations of national security or the prevention of crime specific to the individual or individuals concerned and attended by appropriate and verifiable safeguards: see, by analogy, my comments in relation to Irish constitutional law at paragraphs 52-56 of the judgment.

25. It must be stressed, however, that neither the validity of the 1995 Directive nor the Commission Decision providing for the Safe Harbour Regime are, as such, under challenge in these judicial review proceedings. Nor has it been suggested that Irish law does not accurately reflect Article 25(6) of the 1995 Directive inasmuch as that law provides that the Commissioner is bound by the country-specific findings contained in Safe Harbour Decision of the European Commission as to the adequacy of the data protection regime in the third country.

26. Given what is suggested is the incompatibility *in abstracto* of the Safe Harbour Decision with the requirements of Article 7 and Article 8 of Charter, then the Court may consider that an interpretation of the 1995 Directive in general (and Article 25(6) in particular) along with the 2000 Safe Harbour Decision may be open which would enable a national authority to conduct an investigation of its own in order to ascertain whether the transfer of personal data to a third country satisfies the requirements of Article 7 and Article 8 of the Charter in the light of cases such as *Digital Rights Ireland*.

27. If, however, the Court considers that such an interpretation of the 1995 Directive and the Safe Harbour Decision would be *contra legem* or otherwise not open, then it is suggested that national authorities are entirely bound by the terms of the Safe Harbour Decision. Since there is no suggestion in the present case that either Facebook Ireland or Facebook have

themselves breached the Safe Harbour principles so far as this particular complaint is concerned, it would follow in those circumstances that the conclusion of the Commissioner that this complaint was unsustainable in law would be entirely correct.

Joinder of Digital Rights Ireland Ltd. as *amicus curiae*

28. Following the delivery of my judgment on 18th June, 2014, Digital Rights Ireland Ltd. (“DRI”) applied by notice of motion to be joined to the proceedings as an *amicus curiae*. In a supplementary judgment delivered by me on 16th July, 2014, I acceded to that application: see *Schrems v. Data Protection Commissioner (No.2)* [2014] IEHC 351. A copy of those motion papers, the court order of 16th July, 2014, and a copy of this supplementary judgment is attached as **Appendix 5**.

29. DRI also applied to have additional questions added to the original reference. It was made clear in oral argument in particular that these proposed questions related to the validity of the 1995 Directive and the Safe Harbour Decision itself having regard to Article 8 of the Charter. I took the view that it would be inappropriate to include these suggested questions because they would materially alter the parameters of the proceedings as defined by the parties: see paragraphs 37-41 of the supplementary judgment.

Protective costs order and the applicant

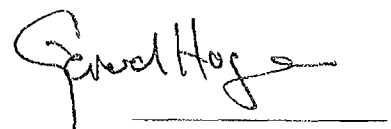
30. By notice of motion dated 4th July, 2014, the applicant applied for a protective costs order limiting his maximum costs exposure vis-à-vis the respondent Commissioner. On 16th July, 2014, I made an order limiting that potential exposure to €10,000. A copy of those motion papers and that order is attached as **Appendix 6**.

Appendix

1. Booklet of judicial review proceedings (including and affidavits) exhibits and court order for reference under Article 267 TFEU.
2. Data Protection Acts 1988-2003 (consolidated version).
3. Judgment of the High Court of 18th June, 2014, *Schrems v. Data Protection Commissioner* [2014] IEHC 310.
4. Judgments of the Irish courts in *Kennedy v. Ireland* [1987] I.R. 587 and *People v. O'Brien* [2012] IECCA 68.
5. Judgment of the High Court of 16th July, 2014, *Schrems v. Data Protection Commissioner (No.2)* [2014] IEHC 351 and motion papers in *amicus curiae* application on the part of Digital Rights Ireland Ltd.
6. Application for protective costs order (including motion papers and affidavits) and court order limiting potential costs exposure of the applicant to €10,000.

Dated 17th July, 2014

Signed

A handwritten signature in black ink, appearing to read 'Gerard Hogan', written over a horizontal line.

Mr. Justice Gerard Hogan

Judge of the High Court of Ireland